PKI-Based Security For P2P Information Sharing

By

Abdelilah Essiari

Karlo Berket, Artur Muratas

Lawrence Berkeley National Lab

Introduction

- Present some of the issues with securing dynamic collaborations in environments where resources and users can cross many trust boundaries.
- Propose solutions and show how they are being used in a P2P file sharing application called scishare.

Traditional Security Model

- Authorized users are predefined.
  - In or out
  - Harder to meet ‘new people’ online in a collaboration.
- Policies are managed by third party entities (administrators).
  - Hard to start a spontaneous collaboration
    - Setup takes time
  - Hard to invite a person to an established collaboration
    - Must contact resource administrators
    - Admins have all the power
- Security becomes a nuisance.
  - Users may resort to un-secure solutions

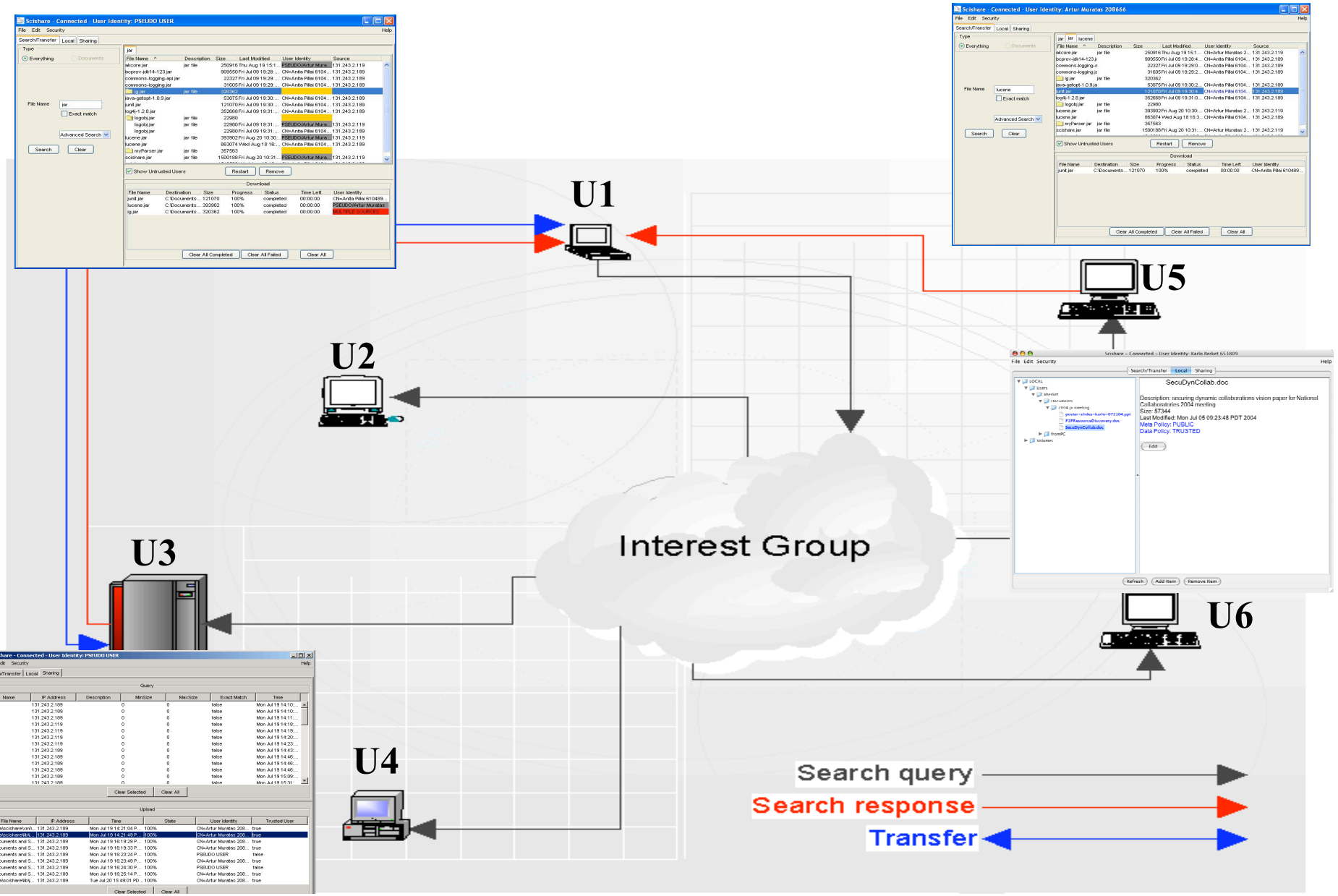
A More Flexible Security Model

- Partition the collaboration into two types of **secure** components:
  - Public
    - Capture users' identities
    - Gradual trust in the collaboration
    - Turn off public components
  - Protected
    - Authorized users only
    - Give invitation/escort powers to some of these users
- Example of components:
    - Communication channels, online instruments, chat rooms, shared spaces, files, …

Approach

- Use Public Key Infrastructure (PKI)
  - X509 certification/online CAs
  - Flexible Trust Models
  - Reduces Key Management issues
- Use existing PKI-based security technologies
  - Modifications are external
  - Reduce the risk of introducing security holes

Scishare Architecture



Components In Scishare

- Unicast channels
  - Managed by the users participating in the communication
- Multicast channel
  - Managed by ‘Third-Party administrators’
- Files and metadata
  - Managed by individual users

Background

- SSL on top of TCP
  - Confidentiality, integrity, authentication
  - Servers ‘must have’ X509 certificates
    - P2P: Every peer plays the role of a server
- SGL on top IGP
  - IGP: decentralized ‘TCP like’ group protocol
  - SGL: decentralized ‘ SSL-like’ group protocol
- Akenti authorization system
  - Capability certificate (resource, user, rights)
  - Push model

Securing Unicast

- Every user can start/connect to a secure server
  - Provide users with pseudo X509 certificates if they don't have any.
  - Trust Managers
    - Accept any valid chain
    - Add un-trusted users to a list accessible by users
    - Users can authorize un-trusted users based on experiences.
  - A single channel can handle both protected and public traffic.
    - Simplifies development

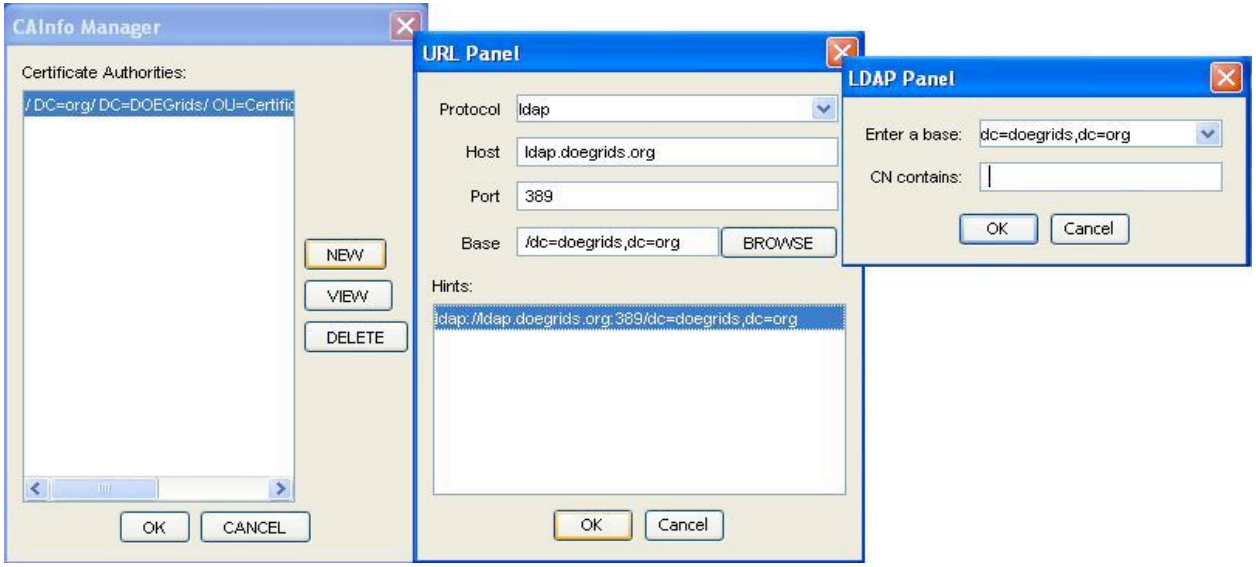
Securing Multicast

- Public group communication channel.
  - Every user can join
- Protected group communication channel.
  - Fine-grained access control
    - Join, invite, escort
    - Capabilities
      - Short lived, signed by the enforcers
    - Invitations/Escorts
      - Short lived, signed by authorized users
- A single communication channel.
  - A protected SGL layer over a public one

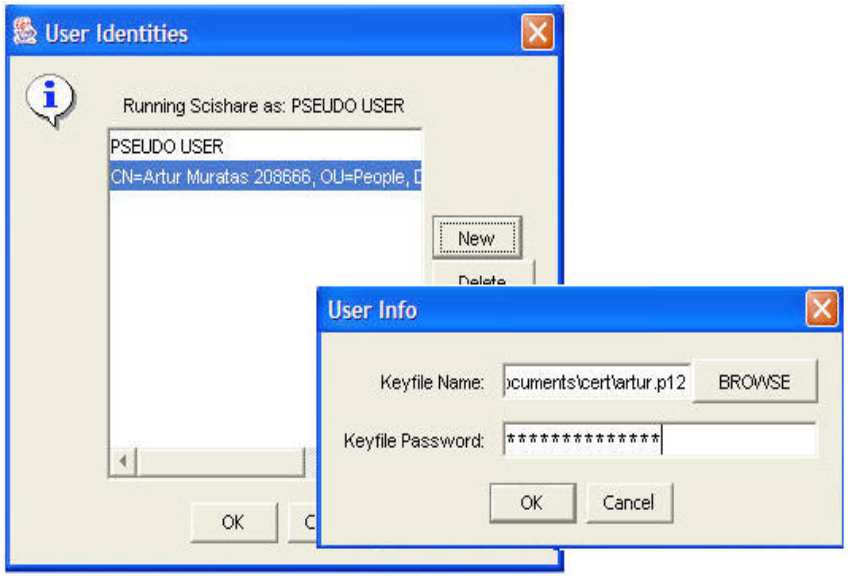
Securing Files and Metadata

- Group-based access control
  - Provide a simple high level interface to users
  - Akenti is used underneath
    - Distributed groups
    - User revocation
    - Future complex expressions
      - Time of day, …

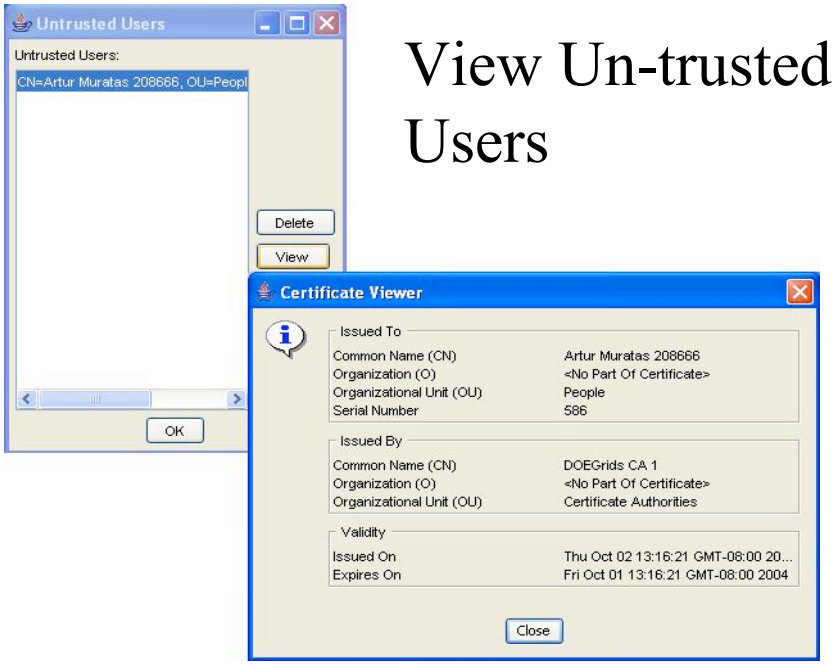
Manage CAs



Manage User Identity

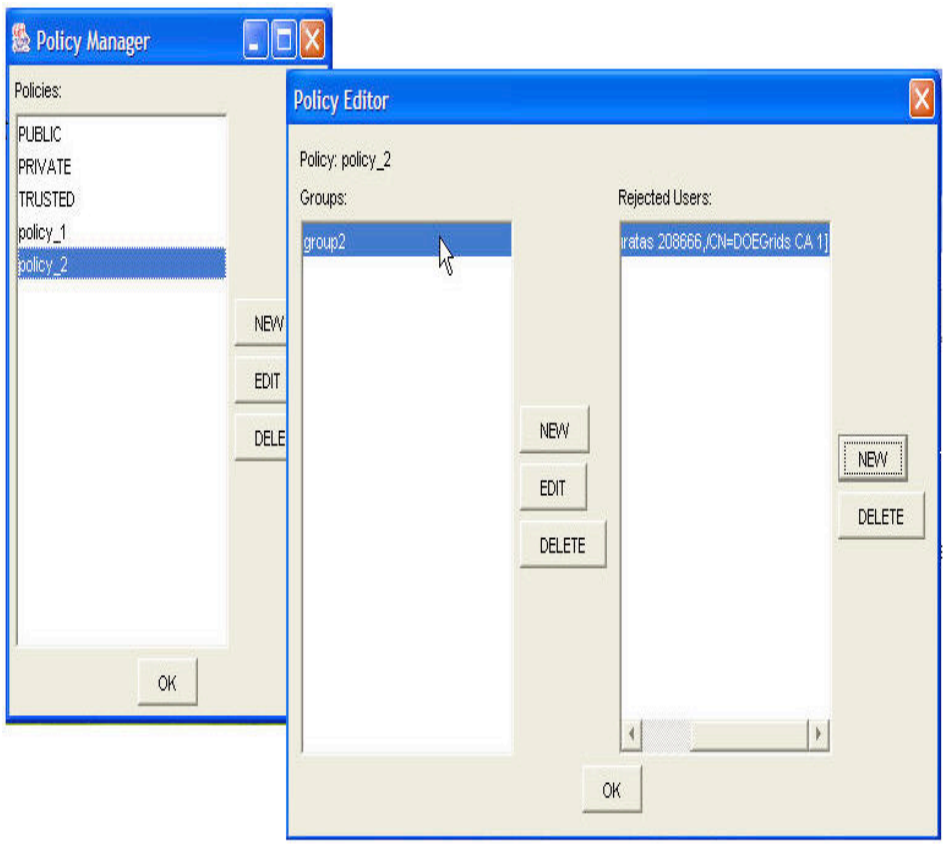


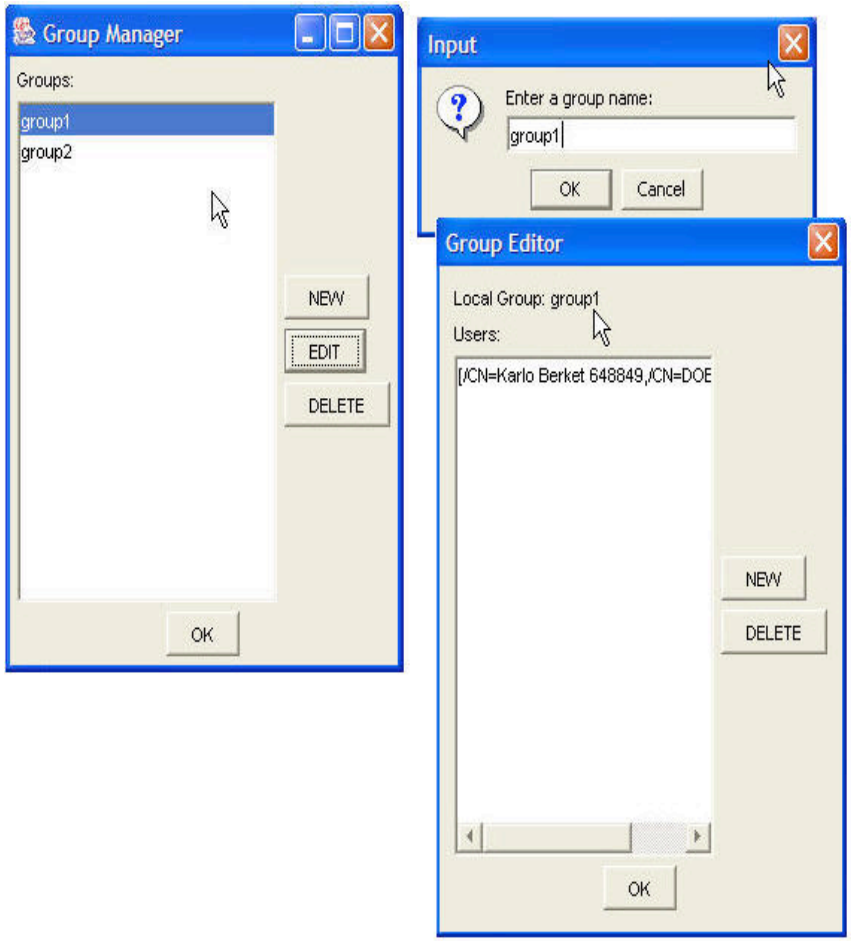
View Un-trusted Users



Manage Policies

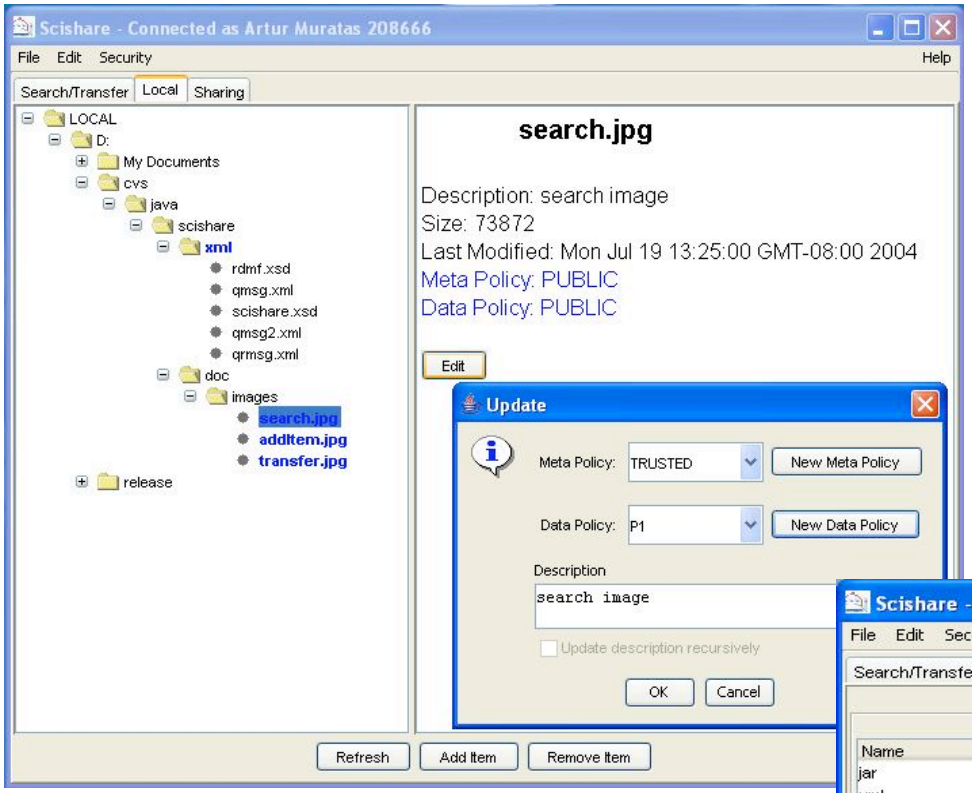
Manage Groups





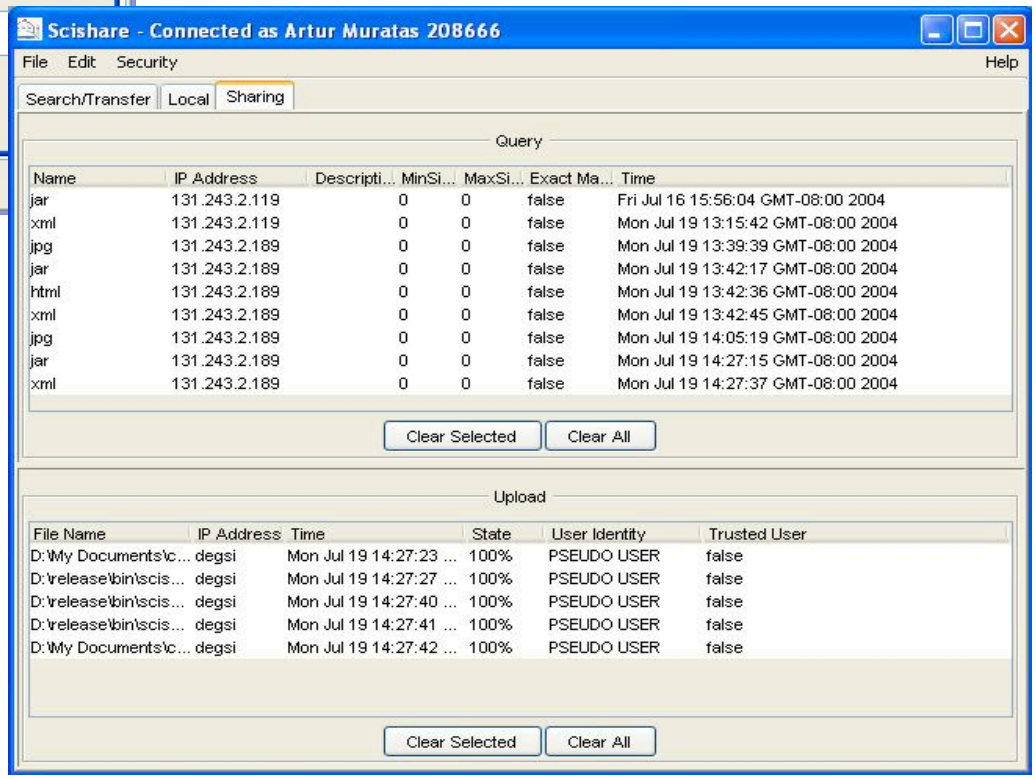
Local

- Add/remove files in DB.
- Map different policies to metadata and data.



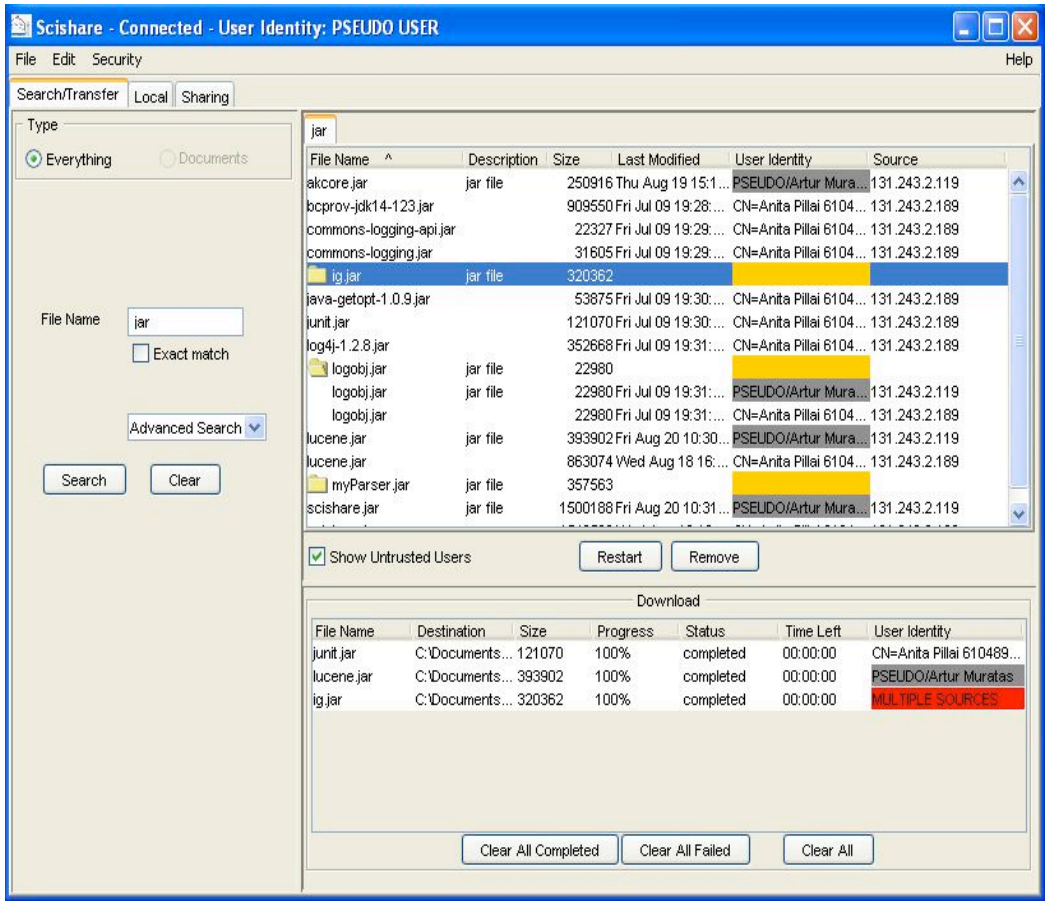
Sharing

- View incoming queries
- View file uploads



Search - Transfer

- Start a search.
- Display the origin of the metadata and its trustworthiness
- Display the origin of the file and its trustworthiness



Future Directions

- Message level security
  - SOAP
- Grid Security Model
  - Virtual organizations
  - X509 proxy certificates/Delegation
  - X509 attribute certificates

Conclusion

- Simple ideas to make secure online collaborations more successful.
- Did not invent any new technology.
- Scishare is out there and every week we are improving it.
- http://www.dsd.lbl.gov